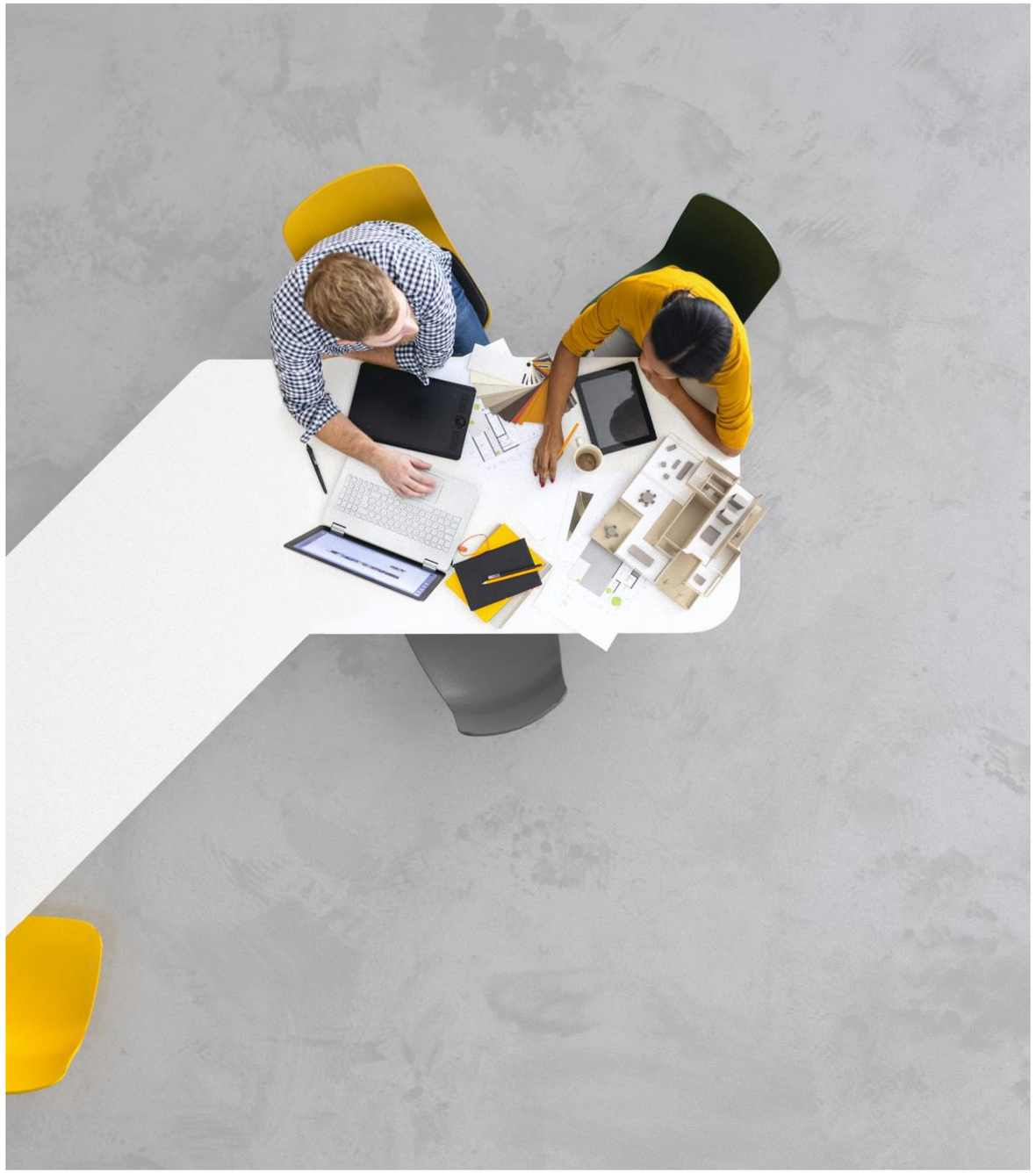
IBM sigurnosna rješenja u eri umjetne inteligencije



Ivan Petrović
Senior Technology Partner Specialist
IBM Quantum Ambassador
ivan.petrovic@hr.ibm.com

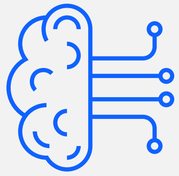
Key cybersecurity priorities impacting the business

Rapid cloud adoption brings new business risk

82% of breaches in 2022 involved data in the cloud, 39% spanned multiple cloud environments[1]

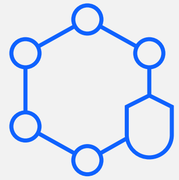
Attackers operate with greater speed and efficiency

AI can generate a deceptive phish in just 5 minutes, a potential time savings of nearly 2 days for attackers[2]



New AI-powered defenses save time and money

Early AI adopters are reducing their total cybersecurity costs by 15% and data breach costs by at least 18%[3]



Shift from point security products to platforms

75% of organizations are pursuing security vendor consolidation according to Gartner's CISO study[4]

[1]IBM Cost of a Data Breach Report 2023; [2]IBM X-Force Threat Intelligence Index 2024; [3]IBM Institute for Business Value: AI and automation for cybersecurity; [4]2022 Gartner's CISO: Security Vendor Consolidation Study

Current SecOps

Technology focused

Dependent on experts and heroes

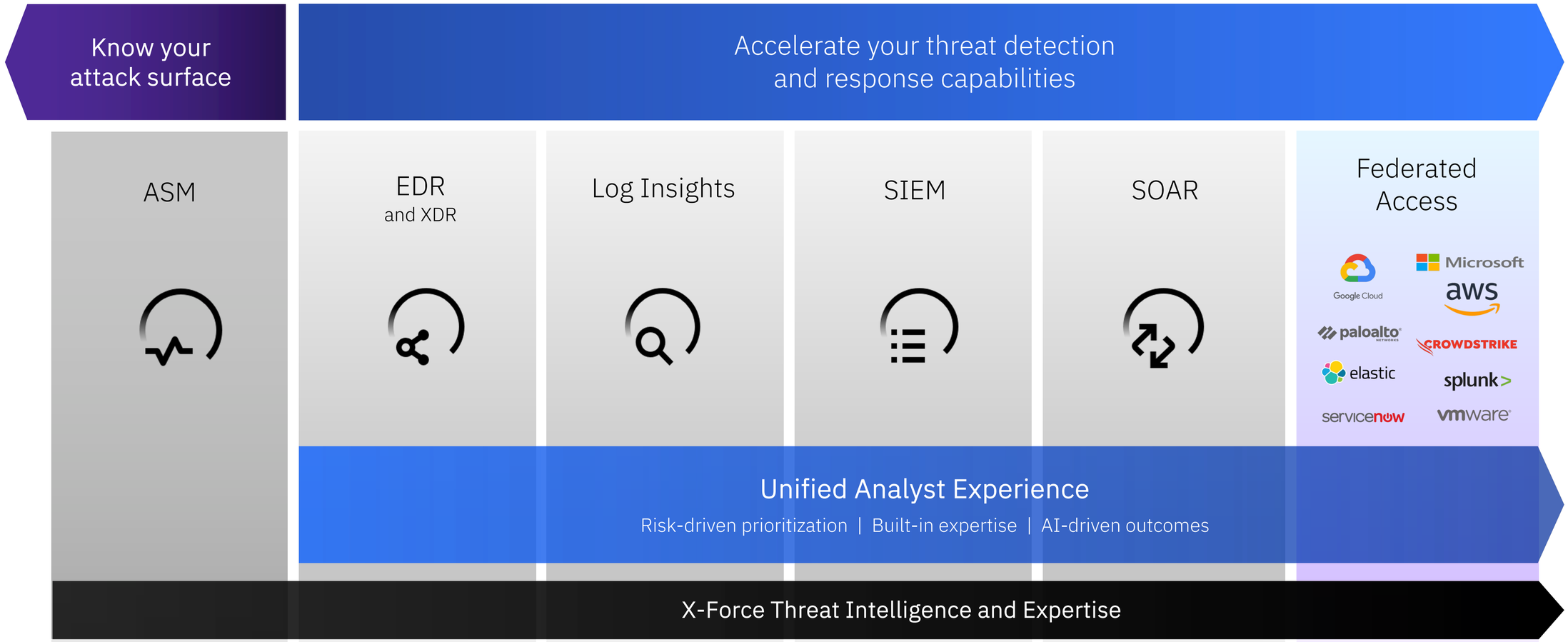
Proprietary ecosystems

Modernized SecOps

- Analyst focused
- Scale with expertise and AI
- Community collaboration

IBM Security QRadar Suite

Predict, prevent, and respond to modern threats



Open Platform. Open Integration. Open Threat Intelligence.

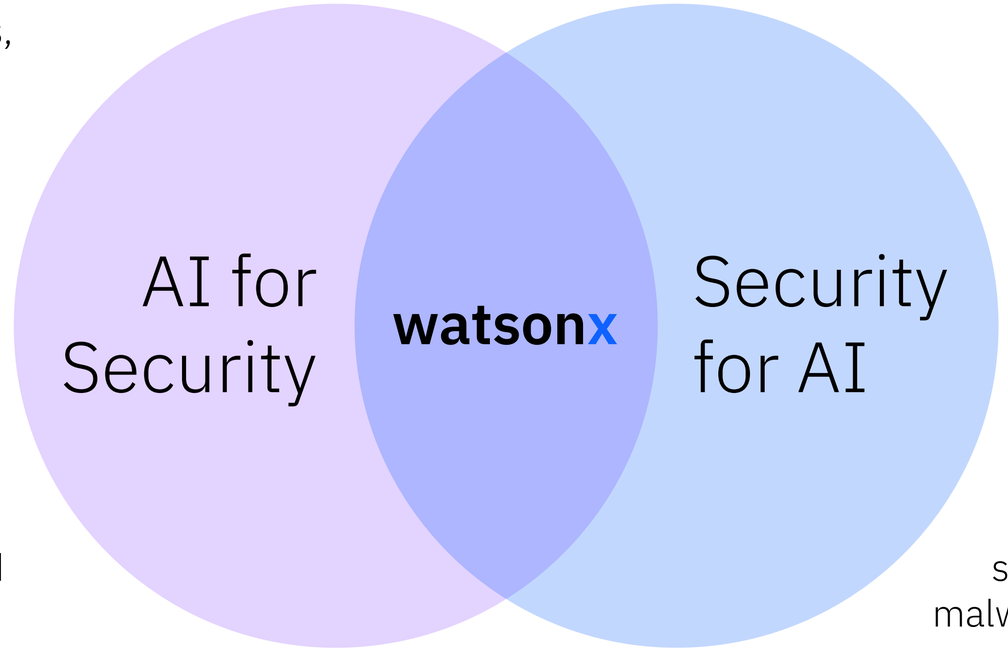
IBM’s Cybersecurity + AI POV

Productivity gains from foundation models and generative AI will reduce human bottlenecks in security

AI will manage repetitive security tasks
such as summarizing alerts and log analysis, freeing teams to tackle strategic problems

AI will generate security content
(detections, workflows, policies) faster than humans, expediting implementation and adjusting to changing security threats in real-time

AI will learn and create active responses
that optimize over time, with abilities to find all similar incidents, update all affected systems, and patch all vulnerable code



Protecting foundation models, generative AI, and their data sets is essential for enterprise-ready AI

Secure the underlying AI training data
by protecting it from sensitive data theft, manipulation, and compliance violations

Secure the usage of AI models
by detecting data or prompt leakage, and alerting on evasion, poisoning, extraction, or inference attacks (IBM Adversarial Robustness Toolkit)

Secure against new AI generated attacks
such as personalized phishing, AI-generated malware, and fake identities by using behavioral defenses and multi-factor authentication

Randori, an IBM Company

Randori Attack Surface Management

The reality of expanding attack surfaces.

30% of assets are unknown or unmanaged due to rapid transformation. (Shadow or Zombie IT)

76% Organizations have been compromised by an unknown or unmanaged asset. [2]

50% By 2026, non-patchable attack surfaces will grow to account for more than half of an enterprise's total exposure. [3]

[1] Forrester Attack Surface Management
[2] 2023 ESG Security Hygiene and Posture Management Remains Decentralized and Complex
[3] Gartner, Implementing A Continuous Threat Exposure Management Program

Common Use Cases to Manage your Expanding Attack Surface

Discover Exposure

Identify your external exposure for full visibility, leveraged to de-risk cloud transformation.

Uncover Shadow IT

Identify your cloud and on-premise assets that are unknown to your organization.

Risk-Based Prioritization

Uplevel vulnerability management with risk-based prioritization and security validation.

Manage M&A Risk

Discover the exposure of subsidiaries to identify risk for mitigation.

Rapid Response

Ability to react swiftly in the event of a security incident.

Exercise Security Program

Build a more resilient program and test your defenses.

How it Works

01

Attack Surface Discovery

- Networks
- Hostnames
- Domains
- IPs

Discovery Validation

- Web Scraping
- Certificate Fingerprinting
- Port Scan
- Artifacts
- Affiliations

02

Exposure Prioritization

- Temptation
- Certificates
- EOL Software
- Open Directory Listing
- Exposed Login
- High Risk Port
- Subdomain Takeover

03

Authorization

04

Continuous Validation

- Initial Access
- Social
- Credentials
- Vulnerability
- Lateral Movement
- Persistence
- Impact

Expert-Driven Engagement

- Human-Led Actions
- Objective Defined Actions

05

Revalidation & Support

- After Action Reports

TARGETING TEAM

ATTACKING TEAM

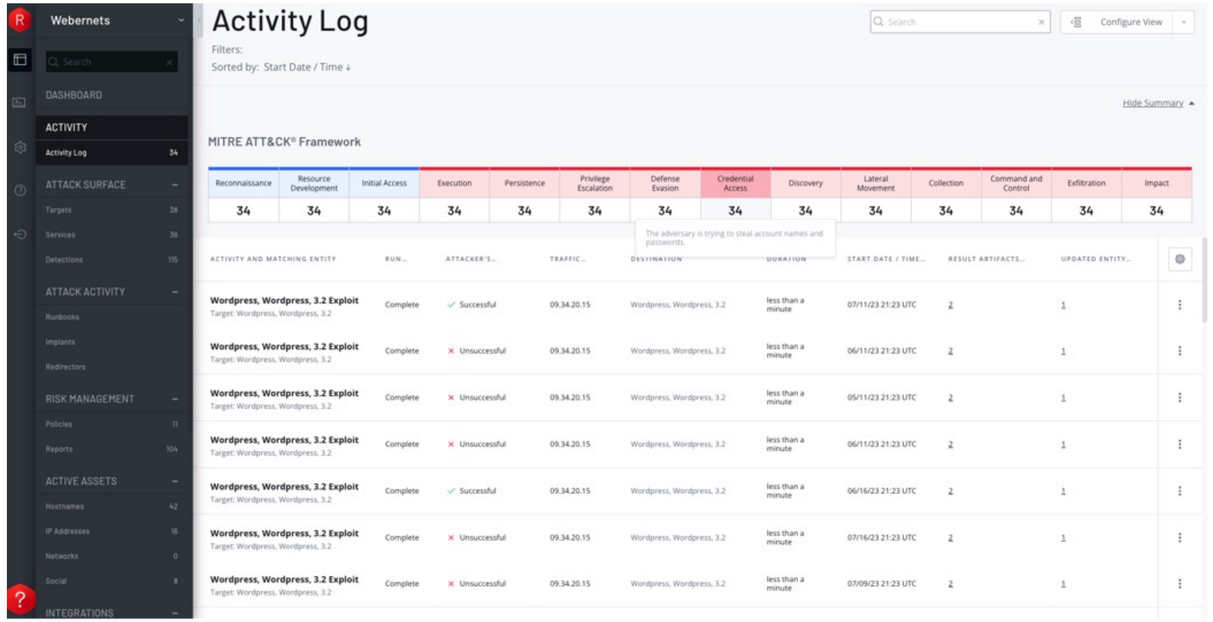
Unified Discovery & Validation

Vulnerability Validation

Ability to verify the existence and exploitability of an identified vulnerability.

– If a vulnerability is successfully exploited this will directly impact the risk-based prioritization scoring resulting in higher relevance and accuracy of temptation.

– Re-test capabilities to identify when a fix is accurately in place to determine time to mitigation.



Activity Log & Library

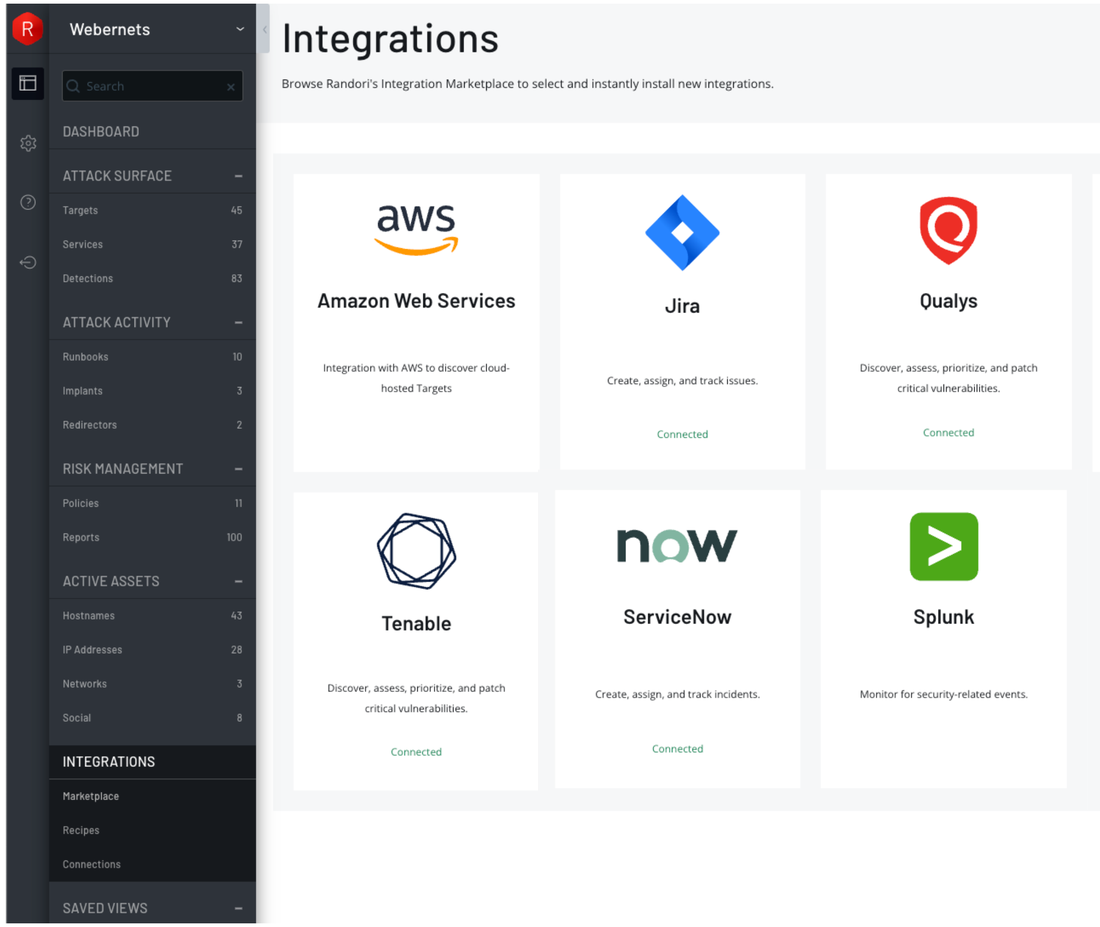
Frictionless Delivery

Integrations Marketplace

Native bi-directional integrations built to operationalize Randori findings.

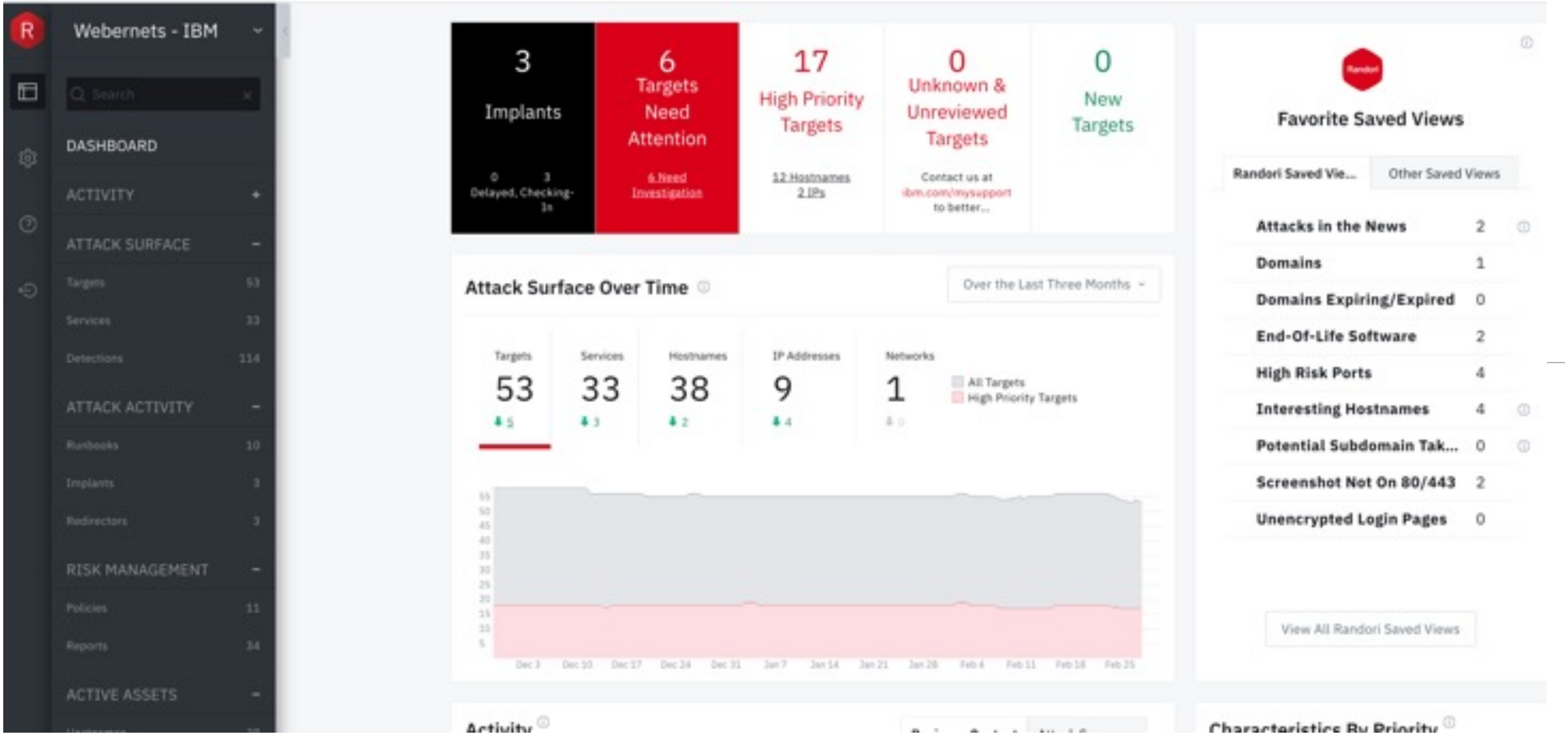
– Eliminate data silos through bi-directional integrations.

– Drive program efficiencies through integrations into vulnerability management.



Open API and Native Integrations

POC and platform look and feel



Customer Success

Randori Recon Onboarding

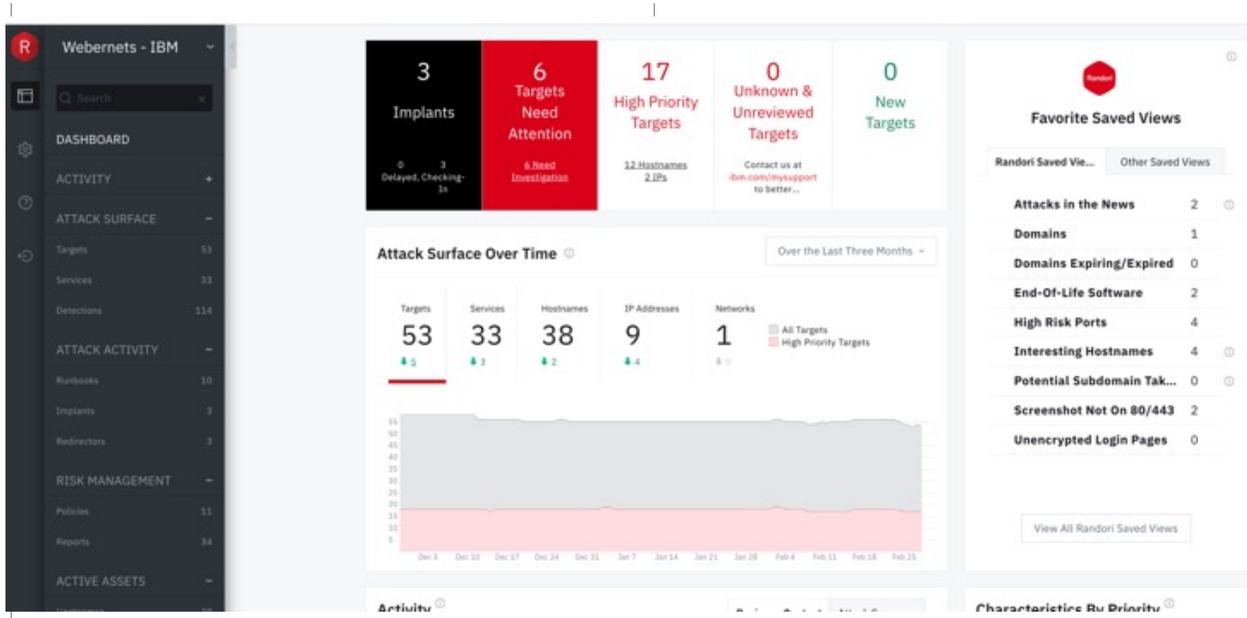
Kickoff Week 0	**Platform Training** Week 1	**Use Case Training** Week 2	**Implementation** Week 3
Activities: • Introductions • Demonstration • Define Goals • Next Steps	Activities: • Randori Discovery • UI Walkthrough • Defining the Attackers Perspective	Activities: • Workflow Features • Randori Customization	Activities: • Plan Workflows • Integrations • Randori Customization
Homework: • Asset Review • KDD 1-2	Homework: • Asset Review • KDD 3	Homework: • KDD 4-6	Homework: • KDD 7-10
Attendees: • Executive Sponsor • Project Lead • Randori Administrators • Randori Champions	Attendees: • Project Lead • Randori Administrators • Randori Champions • All Randori Users	Attendees: • Project Lead • Randori Administrators • Randori Champions • All Randori Users	Attendees: • Project Lead • Randori Administrators • Randori Champions

Continuous Engagement

- Recurring Customer Success Check-Ins
- Executive Business Reviews
- Real-time Communication on Industry Activity
- Ongoing Product Roadmap Input and Updates

Randori Essentials for Service Providers

- Essential offering only
- Partner does all reporting for end client
- Sizing in packages of 1000 employees may be devided in among upto 5 clients
- Each month one client can be changed for new one



Service description:

https://www.ibm.com/support/customer/csol/terms/?id=i126-9757&lc=en